

REMARKS

Claims 1, 3-7 are pending. Claim 2 has been cancelled. Claims 1, 3, 5-7 have been amended to more clearly define the claimed invention.

Claims 1-7 have been rejected under 35 U.S.C. 103 as being unpatentable over Monier in view of Shimbo.

Claim 1, as amended, recites an encryption circuit, comprising:

- a plurality of operation circuits which are connected; and
- a control circuit dividing data to plural parts for providing to each of said plurality of operation circuits and controlling said plurality of operation circuits to provide encryption or decryption control.

Each of said plurality of operation circuits includes:

- a first register holding corresponding part of data as operation data,
- an addition and subtraction circuit performing addition and subtraction with respect to the operation data held in said first register,
- a right-shift circuit performing right-shift with respect to an operation result by said addition and subtraction circuit, and
- a second register holding an operation result by said right-shift circuit.

The claim specifies that:

- the addition and subtraction circuit in a first operation circuit performs addition and subtraction using a carry-in signal supplied from a second operation circuit, and outputs a carry-out signal as said carry-in signal of a third operation circuit; and

-a right-shift circuit in said first operation circuit performs right-shift using a right shift-in signal supplied from said third operation circuit, and outputs a right shift-out signal as said right shift-in signal of said second operation circuit.

Hence, the claim indicates that the claimed encryption circuit has a control circuit and a plurality of operation circuits. Each of the operation circuits includes the addition and subtraction circuit, right-shift circuit, and the first and second registers. The addition and subtraction circuit in one operation circuit (the first operation circuit) outputs the carry-out signal to the addition and subtraction circuit in another operation circuit (the second operation circuit), and the right-shift circuit in the one operation circuit outputs the shift-out signal to the right-shift circuit in the other operation circuit (the third operation circuit). Hence, the plurality of operation circuits cooperates using the carry-out signal and the shift-out signal.

The Monier and Shimbo references disclose the encryption/decryption circuit for calculating the RSA operation. However, both of these references disclose only a single operation circuit, not a plurality of operation circuits, as claim 1 requires.

The operation circuit disclosed in the references performs the loop operation for encrypting the initial data, and the carry-out signal and/or shift-out signal is transferred to the proceeding operation.

Hence, both references do not suggest using a plurality of operation circuits for encrypting the corresponding part of data, and cannot suggest that the carry-out signal and/or the shift-out signal of one operation circuit is transferred to another operation circuit.

Recent Examination Guidelines and decisions of the USPTO Board of Appeal and Interferences in *Ex parte Smith*, Appeal 2007-1925 (June 25, 2007) and *Ex parte Catan*, Appeal 2007-0820 (July 3, 2007) that follow the Supreme Court's decision in *KSP Int'l Co. v. Teleflex*

Inc., 127 S.Ct. 17127 (2007) put forth an obviousness analysis that emphasizes a functional approach based on *Graham v. John Deere* factors. As stated in *Graham v. John Deere Co.* 383 U.S. 1, 13, 148 U.S.P.Q. 459, 465 (1966), obviousness under 35 U.S.C. §103 must be determined by (1) analyzing the scope and content of the prior art; (2) ascertaining the differences between the prior art and the claims in issue; (3) resolving the level of ordinary skill in the pertinent art, and (4) analyzing secondary considerations.

As demonstrated above, the subject matter of claim 1 substantially differs from the combined teachings of Monier and Shimbo.

Moreover, the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art. *Cable Electric Products, Inc. v. Genmark, Inc.*, 770 F.2d 1015, 226 USPQ 881 (Fed. Cir. 1985). In determining whether a case of prima facie obviousness exists, it is necessary to ascertain whether the prior art teachings appear to be sufficient to one of ordinary skill in the art to suggest making the claimed substitution or other modification. *In re Lulu*, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1984).

As explained above, the combined teachings of the references are not sufficient to suggest the claimed encryption arrangement involving a plurality of operation circuits, where a carry-out and/or shift-out signal is transferred from one operation circuit to another, as claim 1 requires.

Accordingly, the subject matter of claim 1 is not obvious over the combined teachings of Monier and Shimbo.

Claims 3-7 are defined over the prior art at least for the reasons presented above in connection with claim 1.

In view of the foregoing, and in summary, claims 1 and 3-7 are considered to be in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Alexander V. Yampolsky
Registration No. 36,324

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 AVY:apr
Facsimile: 202.756.8087
Date: January 3, 2008

**Please recognize our Customer No. 20277
as our correspondence address.**